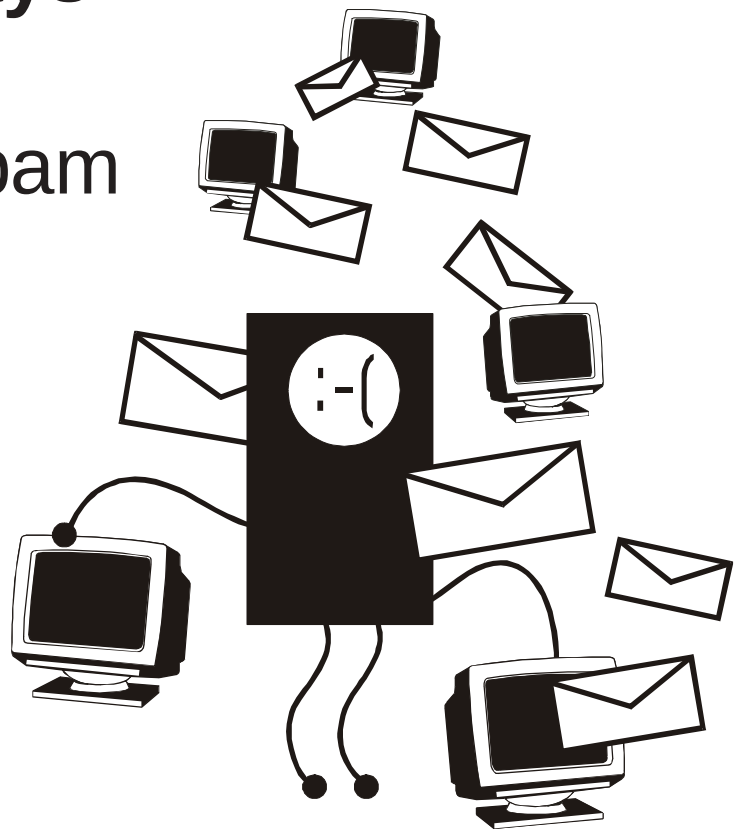
BUSINESS
FOR THE CONSUMER
www.ftc.gov
FEDERAL TRADE COMMISSION
1-877-FTC-HELP

FTC FACTS for Business

Open Relays — Close the Door on Spam



Introduction

Your organization probably handles lots of email every day — both to and from your clients and customers. But did you know that the settings of your mail server may make your system vulnerable to misuse? If your mail server maintains an open door to the Internet, known as an "open relay," someone could access it and pass spam (unsolicited commercial email) through it. Not only could this overload your server but worse still, it could damage your reputation because it will appear that you sent the spam. The Federal Trade Commission (FTC) has brought cases against those that send deceptive commercial spam. As the nation's only general jurisdiction consumer protection agency, the FTC offers these suggestions to help you protect your computer system and the goodwill of your enterprise.

What's the problem?

To understand how mail can be passed through — or "relayed" — by your mail server, keep in mind how email works. To send or receive email, your computer must be connected to a mail server. A mail server is a machine connected to the Internet that runs software allowing it to process email. When you send an email message from a secure server, software in one part of the mail server checks to be sure you're listed as a user within your organization. If so, it sends out your mail. When someone sends *you* an email, software in another part of the server confirms that you're an authorized user, and then accepts and delivers the email to you.

If the server is not secure and some of its settings allow it to stay "open," it will forward email to addressees who are not listed as users in your organization. Often called "open relays," "insecure relays," or "third-party relays," such open mail servers are configured to accept and transfer email on behalf of any user anywhere, including unrelated third parties. The open relay in your email server allows any email sender anywhere to pass messages through your server and onto the ultimate recipients. There is little, if any, benefit to you in allowing this email to cut through your server; the people in your organization aren't receiving or sending it.

How does your server get caught up in this? In the early days of the Internet, many mail servers were kept open to allow email to travel among different networks. This helped the Internet grow. But today, an open relay is most likely to be used by a spammer. Using automated software, spammers scan the Internet for an open relay. If they find out that your server is open, they route their bulk email through it, spamming in greater volume and less time than they could using their own individual computers. Using an open relay lets spammers conceal their identities because it appears that the spam actually comes from you. Recipients of the spam could then flood *your* server with complaints. The spam and resulting email traffic could overwhelm your system. If your server crashes from this overload, repairing it could be costly and time-consuming. Even more costly is the potential loss of goodwill from those who think you've sent the spam. If you're maintaining an open relay, you're leaving your door open to the theft of your computer services and creating the impression that you're sending unwanted junk mail.

And that's not all...

Your mail server could have other vulnerabilities. Maintaining an "open proxy" also opens your mail server to abuse. A proxy server runs software that allows it to be the one machine in your network that directly interacts with the Internet, providing the network with greater security. But if a proxy is not configured properly (an "open proxy"), it also may allow others to pass through your site and connect to other hosts on the Internet. For example, a spammer can use an open proxy to connect to your mail server. If your server is an open mail relay, the spammer can send loads of spam, and then disconnect — all anonymously.

Fixing the problem

To find out whether you have an open relay on your system, check the Mail Transfer Agent software (MTA) your company uses to manage its email. Checking for open relaying and securing your email system against unauthorized use can usually be done with a couple of commands.

A search for anti-spam resources (such as "stop third-party mail relay") on your favorite Internet search engine will reveal resources for securing your server. One good resource for checking your site and learning how to secure

your mail server is the MAPS Transport Security Initiative (TSI), at www.mail-abuse.org/tsi/. You'll find links under "How Can I Fix the Problem?" with tips for many operating systems and the email programs they support. Locate your email program to find detailed instructions on how to secure your email server.

Many resources on the Internet will test whether your proxy is open. Make sure that your systems and network administrators are aware that you're doing proxy tests. A search for anti-spam resources (such as "open proxy") on your favorite Internet search engine will reveal those resources.

Your opportunity to comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to www.sba.gov/ombudsman.

The FTC works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them. To file a complaint or to get free information on consumer issues, visit www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

FEDERAL TRADE COMMISSION | FOR THE CONSUMER
1-877-FTC-HELP | www.ftc.gov

May 2003